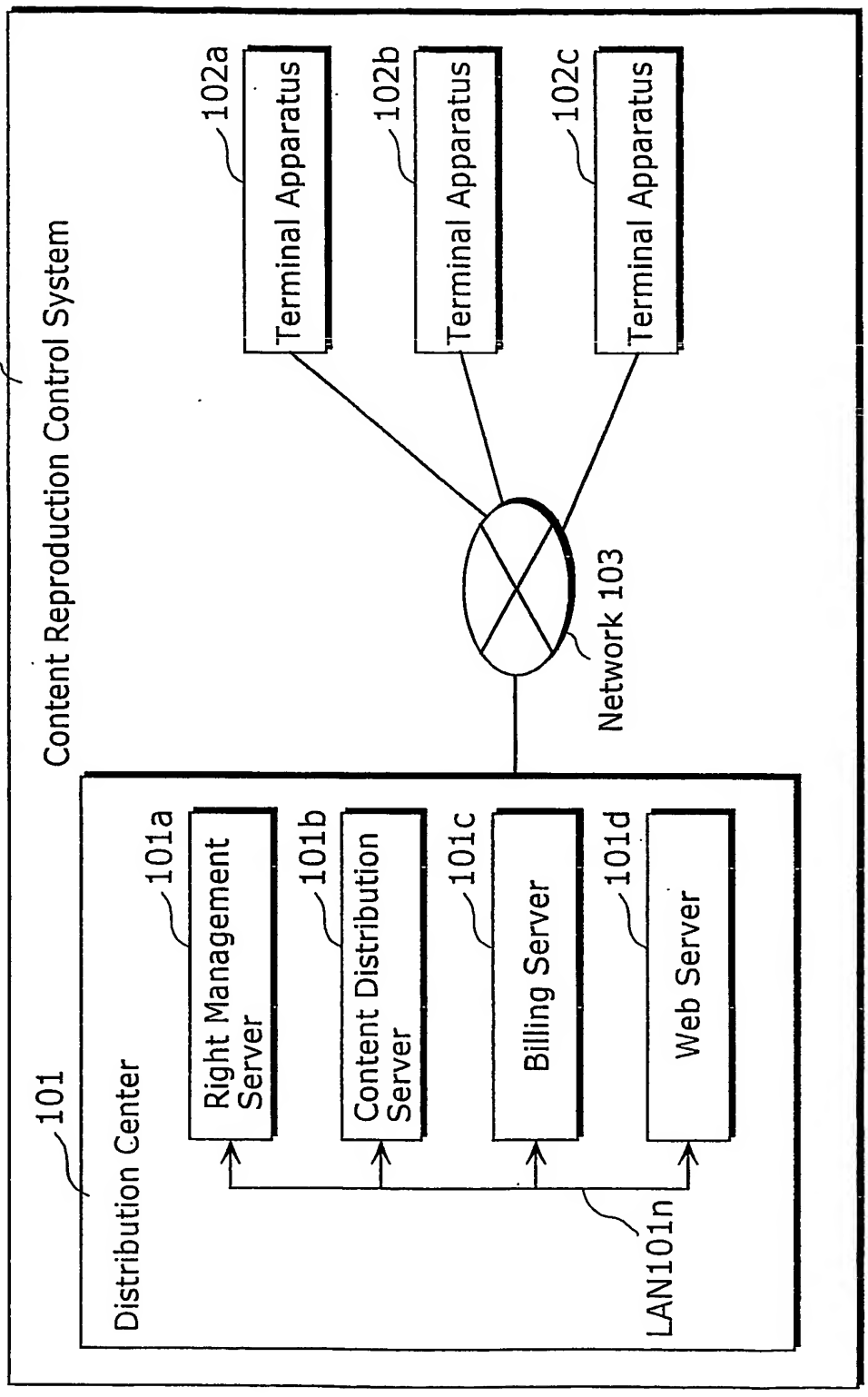
FIG. 1



Best Available Copy

FIG. 2

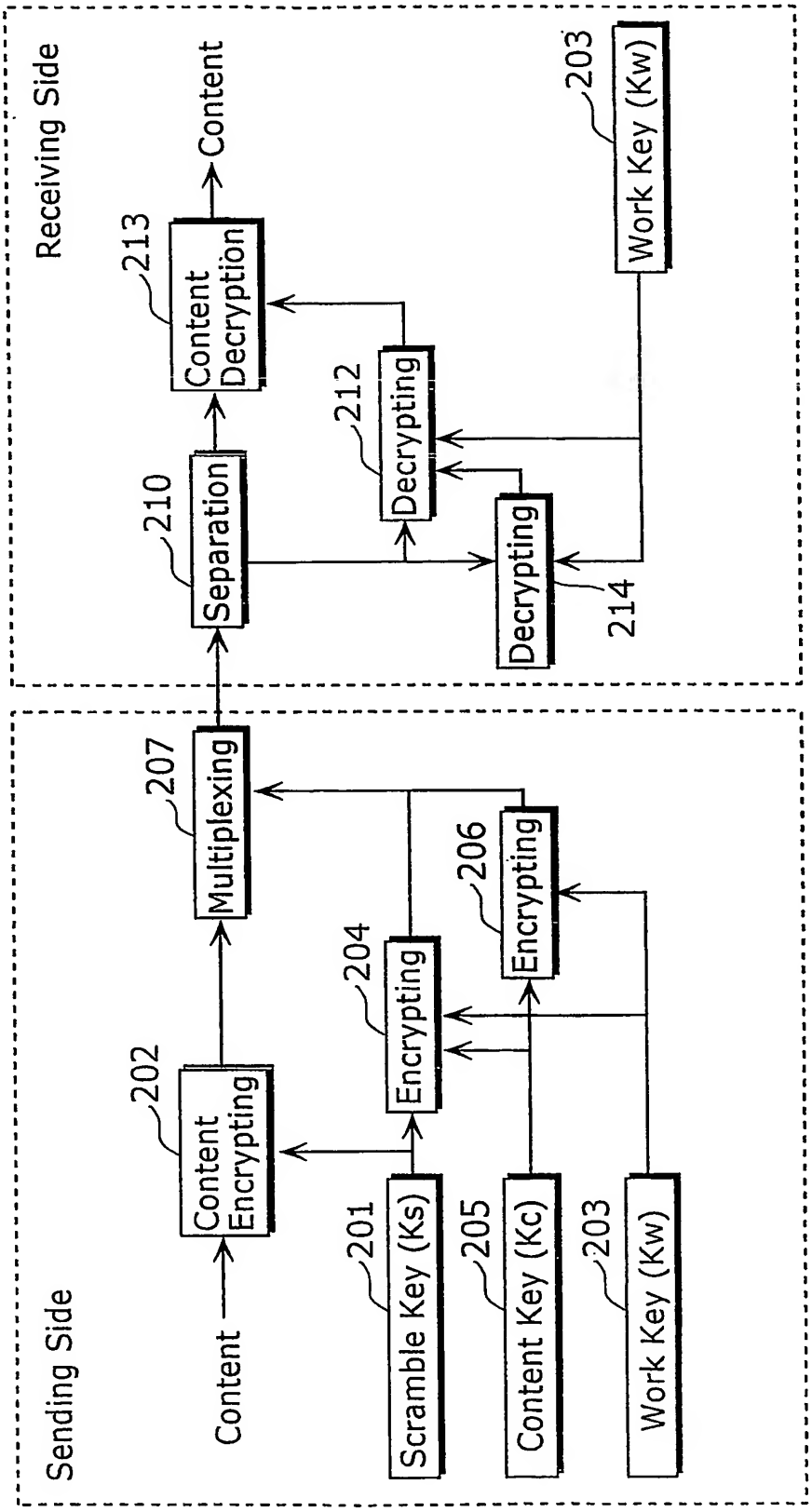

Sending Side
Content
202
Content Encrypting
201
Scramble Key (Ks)
204
Encrypting
205
Content Key (Kc)
206
Encrypting
203
Work Key (Kw)
207
Multiplexing
Receiving Side
210
Separation
212
Decrypting
214
Decrypting
213
Content Decryption
Content
203
Work Key (Kw)

FIG. 3

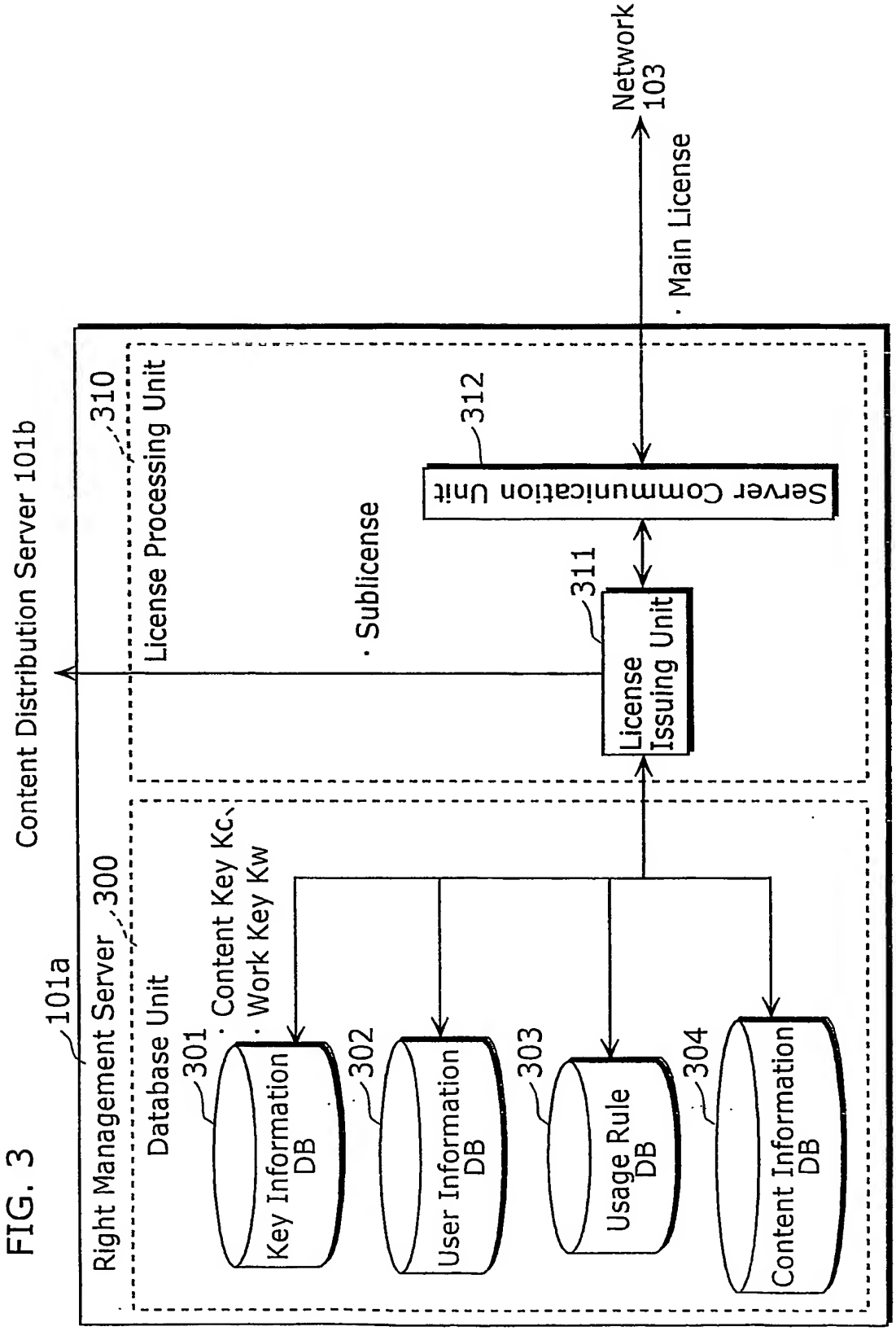

Content Distribution Server 101b
Right Management Server 101a
300
Database Unit
· Content Key Kc
· Work Key Kw
301
Key Information DB
302
User Information DB
303
Usage Rule DB
304
Content Information DB
310
License Processing Unit
311
License Issuing Unit
312
Server Communication Unit
· Sublicense
· Main License
Network 103

FIG. 4

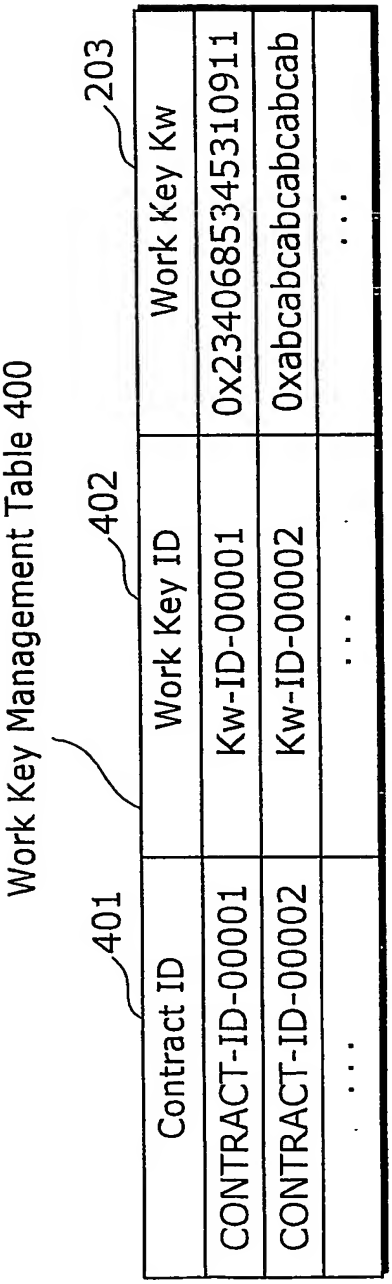

Work Key Management Table 400
401
402
203
Contract ID
Work Key ID
Work Key Kw
CONTRACT-ID-00001
Kw-ID-00001
0x2340685345310911
CONTRACT-ID-00002
Kw-ID-00002
0xabcabcabcabcabcab
. . .
. . .
. . .

FIG. 5

Content Key Management Table 500

501 Content ID	205 Content Key Kc
CONTENT-ID-00001	0x1234567890abcdef
CONTENT-ID-00002	0x43195745a4098b4e
CONTENT-ID-00003	0x3970584ad3922247
CONTENT-ID-00004	0x2411197120121974
. . .	. . .

FIG. 6

User Information Management Table 600

601 User ID	602 Terminal ID
USER-ID-00001	TERMINAL-ID-00001
USER-ID-00002	TERMINAL-ID-12345 TERMINAL-ID-54321
USER-ID-00003	TERMINAL-ID-77777
USER-ID-00004	TERMINAL-ID-99999
. . .	. . .

FIG. 7

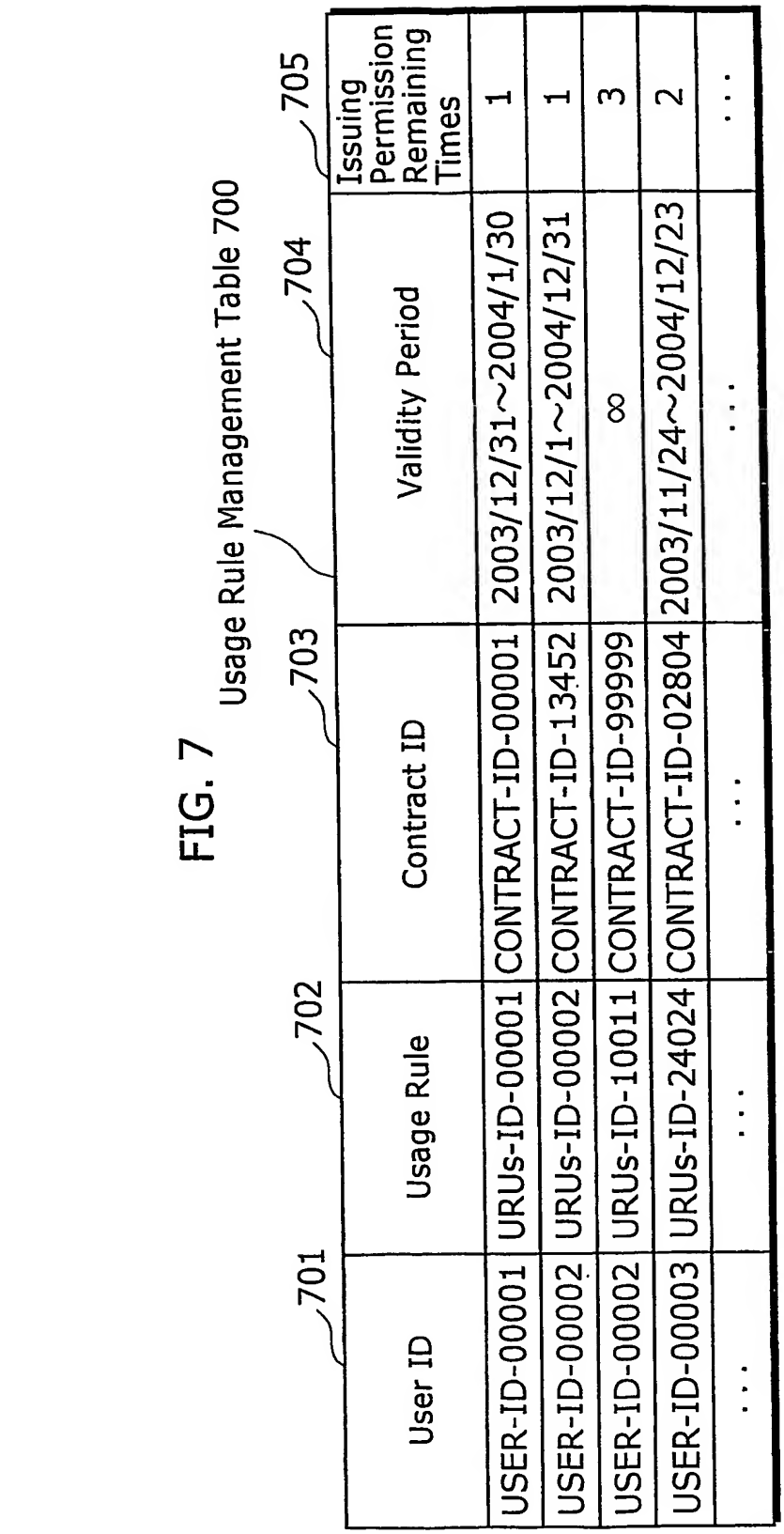

Usage Rule Management Table 700
701
User ID
702
Usage Rule
703
Contract ID
704
Validity Period
705
Issuing Permission Remaining Times
USER-ID-00001
URUs-ID-00001
CONTRACT-ID-00001
2003/12/31~2004/1/30
1
USER-ID-00002
URUs-ID-00002
CONTRACT-ID-13452
2003/12/1~2004/12/31
1
USER-ID-00002
URUs-ID-10011
CONTRACT-ID-99999
∞
3
USER-ID-00003
URUs-ID-24024
CONTRACT-ID-02804
2003/11/24~2004/12/23
2
. . .
. . .
. . .
. . .
. . .

FIG. 8

Content Information Management Table 800

801 Content ID	802 License ID	803 Validity Period	804 Use Permission Times
CONTENT-ID-00001	LICENSE-ID-00001	2003/12/31~2004/1/30	∞
CONTENT-ID-00002	LICENSE-ID-00002	2003/12/1~2004/12/31	∞
CONTENT-ID-00003	LICENSE-ID-00003	∞	1
CONTENT-ID-00004	LICENSE-ID-00004	2003/11/24~2004/12/23	5
...	...	...	...

FIG. 9

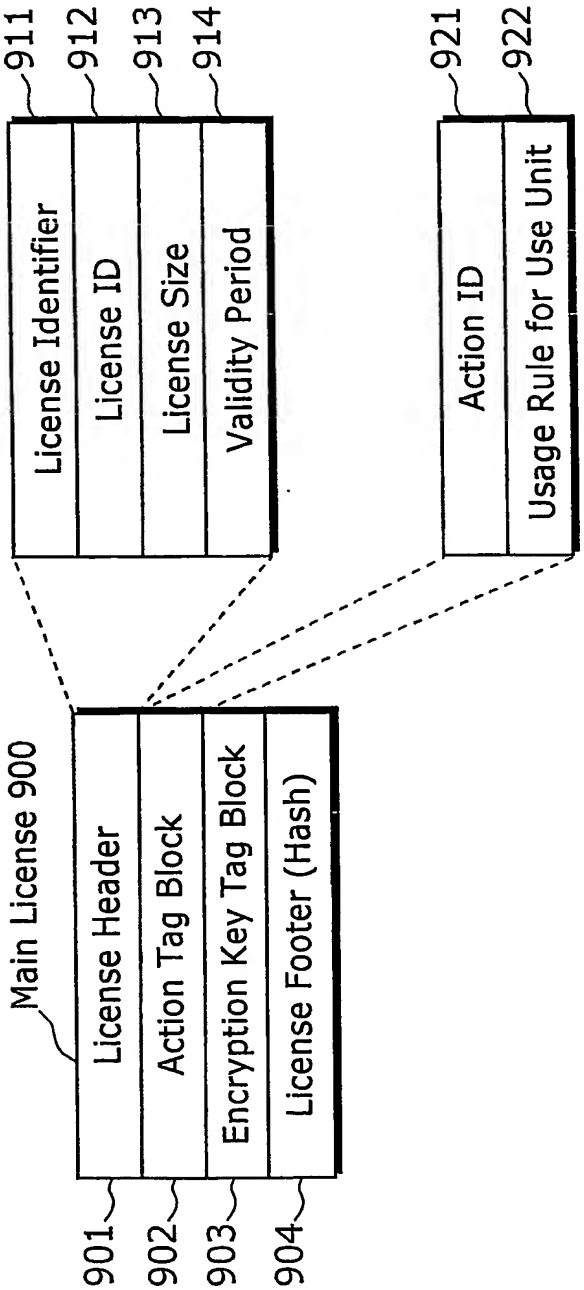

Main License 900
License Header
Action Tag Block
Encryption Key Tag Block
License Footer (Hash)
901
902
903
904
License Identifier
License ID
License Size
Validity Period
911
912
913
914
Action ID
Usage Rule for Use Unit
921
922

FIG. 10

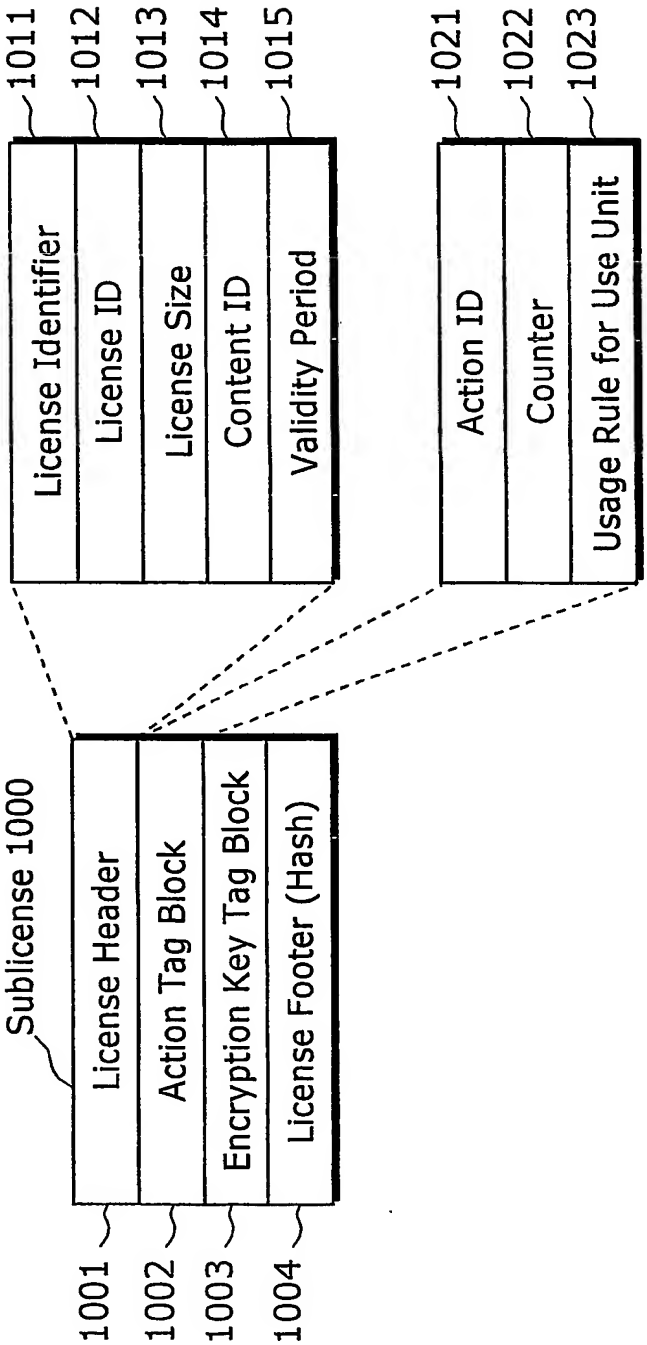

Sublicense 1000
License Header
Action Tag Block
Encryption Key Tag Block
License Footer (Hash)
1001
1002
1003
1004
License Identifier
License ID
License Size
Content ID
Validity Period
1011
1012
1013
1014
1015
Action ID
Counter
Usage Rule for Use Unit
1021
1022
1023

FIG. 11

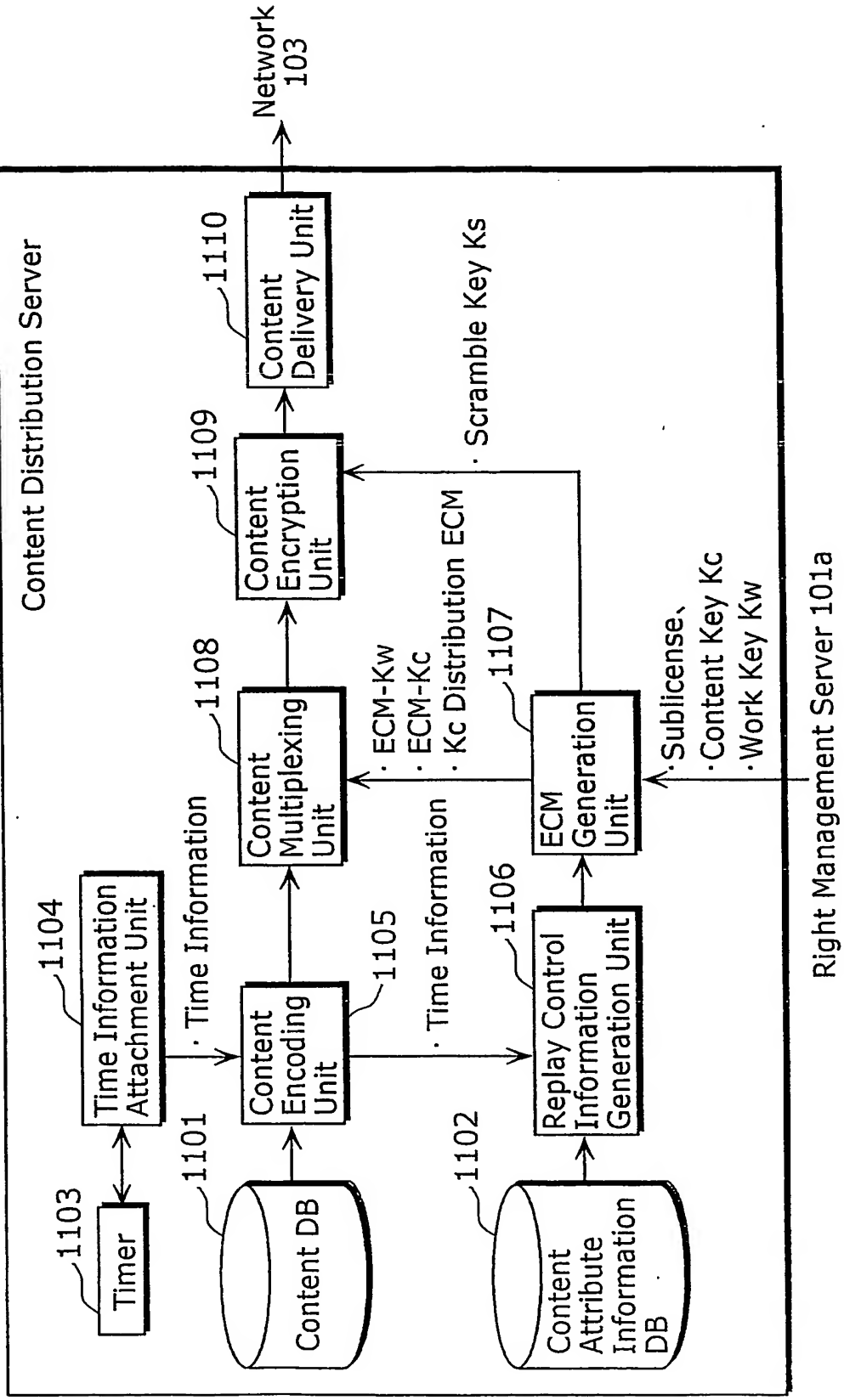

101b
Content Distribution Server
Network 103
1110
Content Delivery Unit
1109
Content Encryption Unit
· Scramble Key Ks
1108
Content Multiplexing Unit
· ECM-Kw
· ECM-Kc
· Kc Distribution ECM
1107
ECM Generation Unit
· Sublicense,
· Content Key Kc
· Work Key Kw
Right Management Server 101a
1104
Time Information Attachment Unit
· Time Information
1105
Content Encoding Unit
· Time Information
1106
Replay Control Information Generation Unit
1103
Timer
1101
Content DB
1102
Content Attribute Information DB

FIG. 12

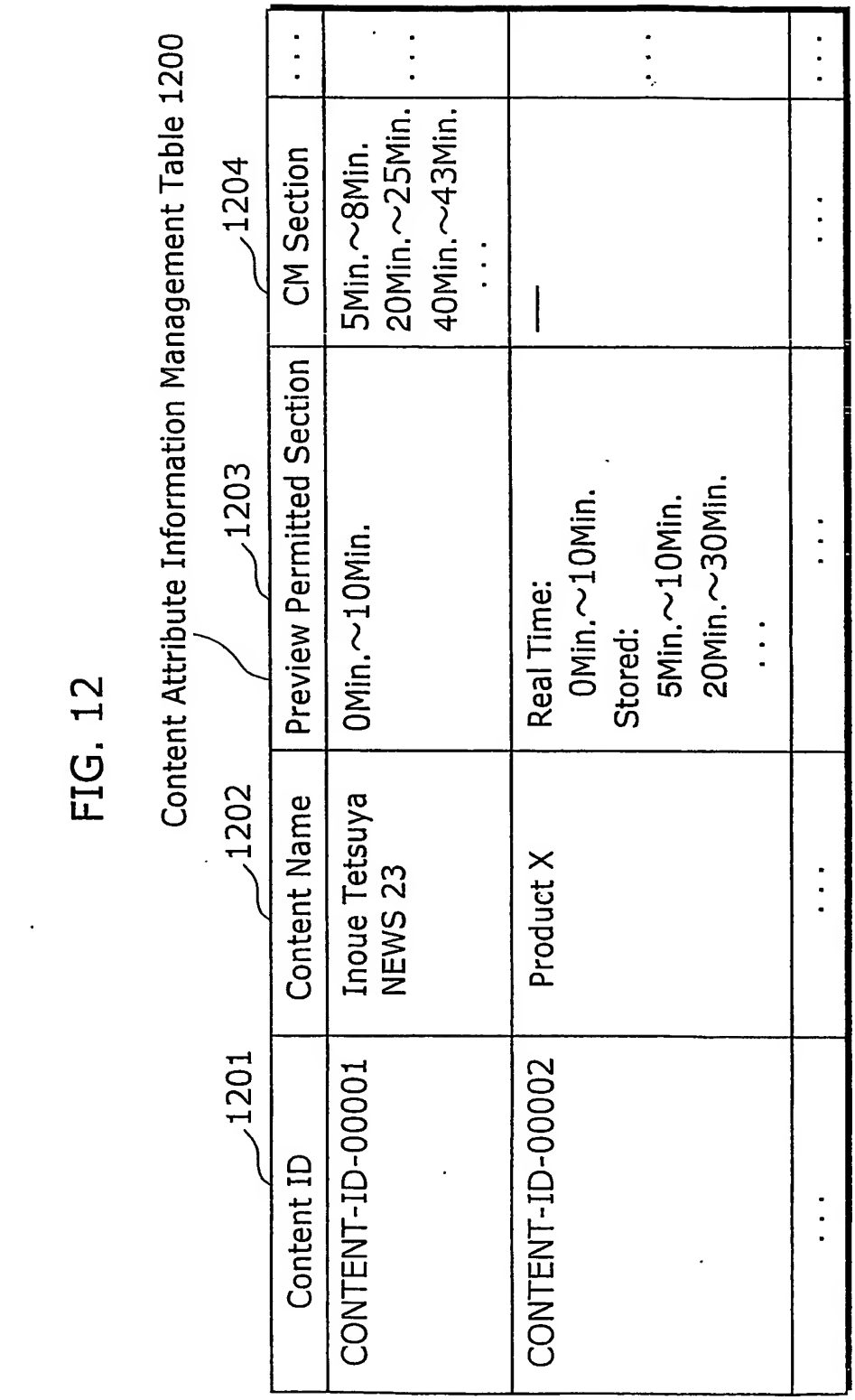

Content Attribute Information Management Table 1200
1201
1202
1203
1204
Content ID
Content Name
Preview Permitted Section
CM Section
CONTENT-ID-00001
Inoue Tetsuya NEWS 23
0Min.~10Min.
5Min.~8Min.
20Min.~25Min.
40Min.~43Min.
CONTENT-ID-00002
Product X
Real Time:
0Min.~10Min.
Stored:
5Min.~10Min.
20Min.~30Min.
—

FIG. 13

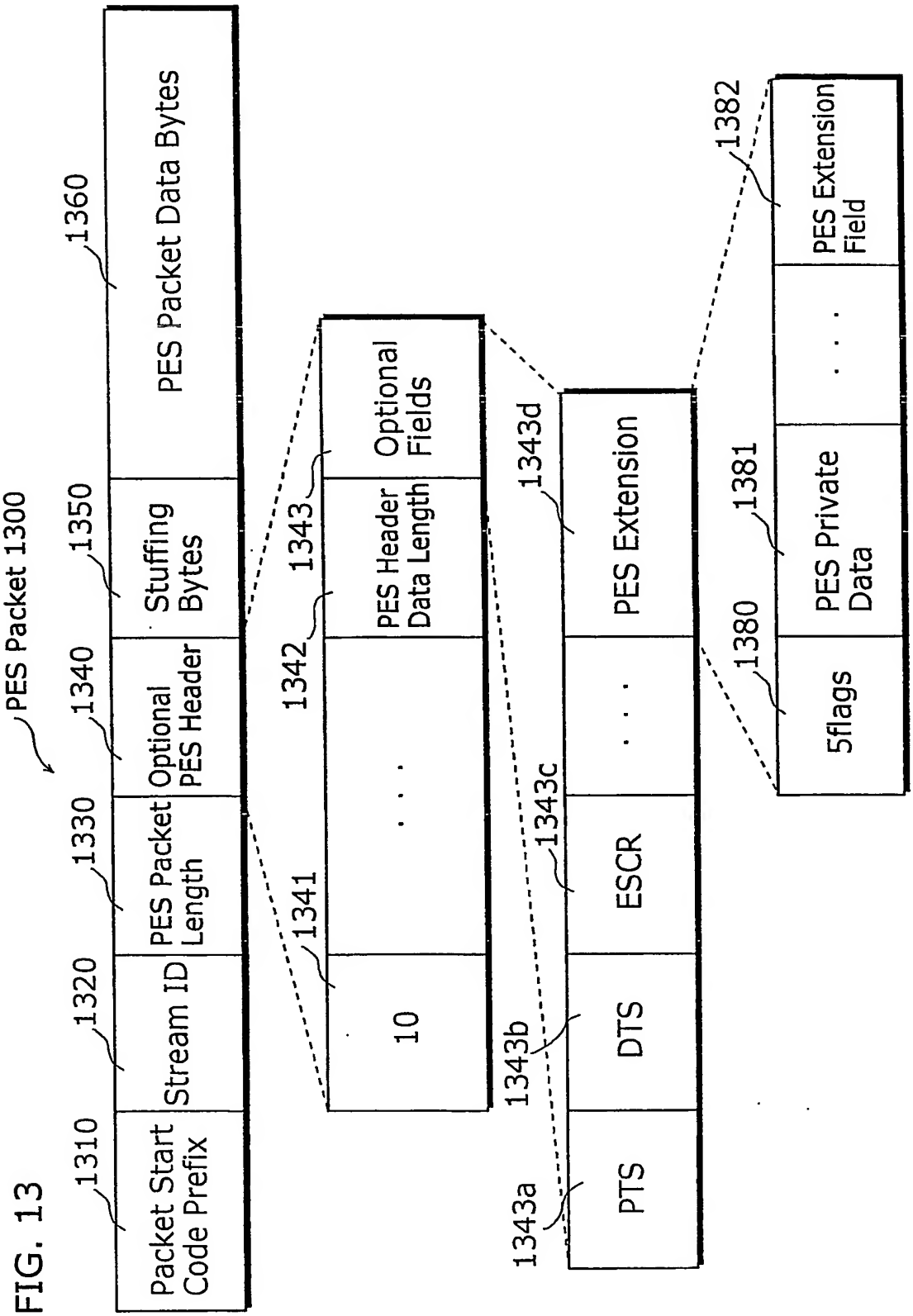

PES Packet 1300
1310
Packet Start Code Prefix
1320
Stream ID
1330
PES Packet Length
1340
Optional PES Header
1350
Stuffing Bytes
1360
PES Packet Data Bytes
1341
10
1342
. . .
1343
PES Header Data Length
Optional Fields
1343a
PTS
1343b
DTS
1343c
ESCR
1343d
. . .
PES Extension
1380
5flags
1381
PES Private Data
1382
. . .
PES Extension Field

FIG. 14

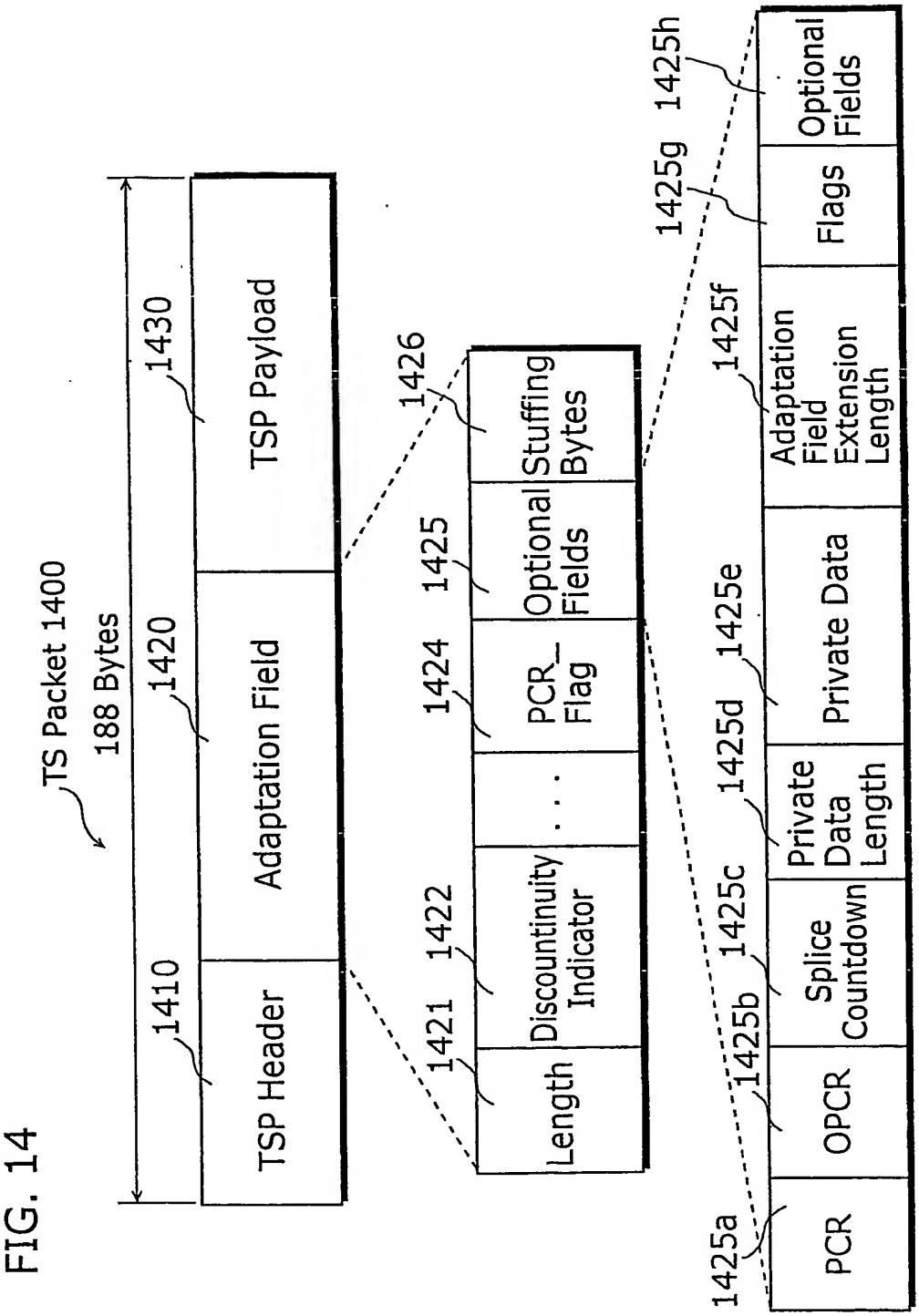

TS Packet 1400
188 Bytes
1410
TSP Header
1420
Adaptation Field
1430
TSP Payload
1421
Length
1422
Discountinuity Indicator
. . .
1424
PCR_ Flag
1425
Optional Fields
1426
Stuffing Bytes
1425a
PCR
1425b
OPCR
1425c
Splice Countdown
1425d
Private Data Length
1425e
Private Data
1425f
Adaptation Field Extension Length
1425g
Flags
1425h
Optional Fields

FIG. 15

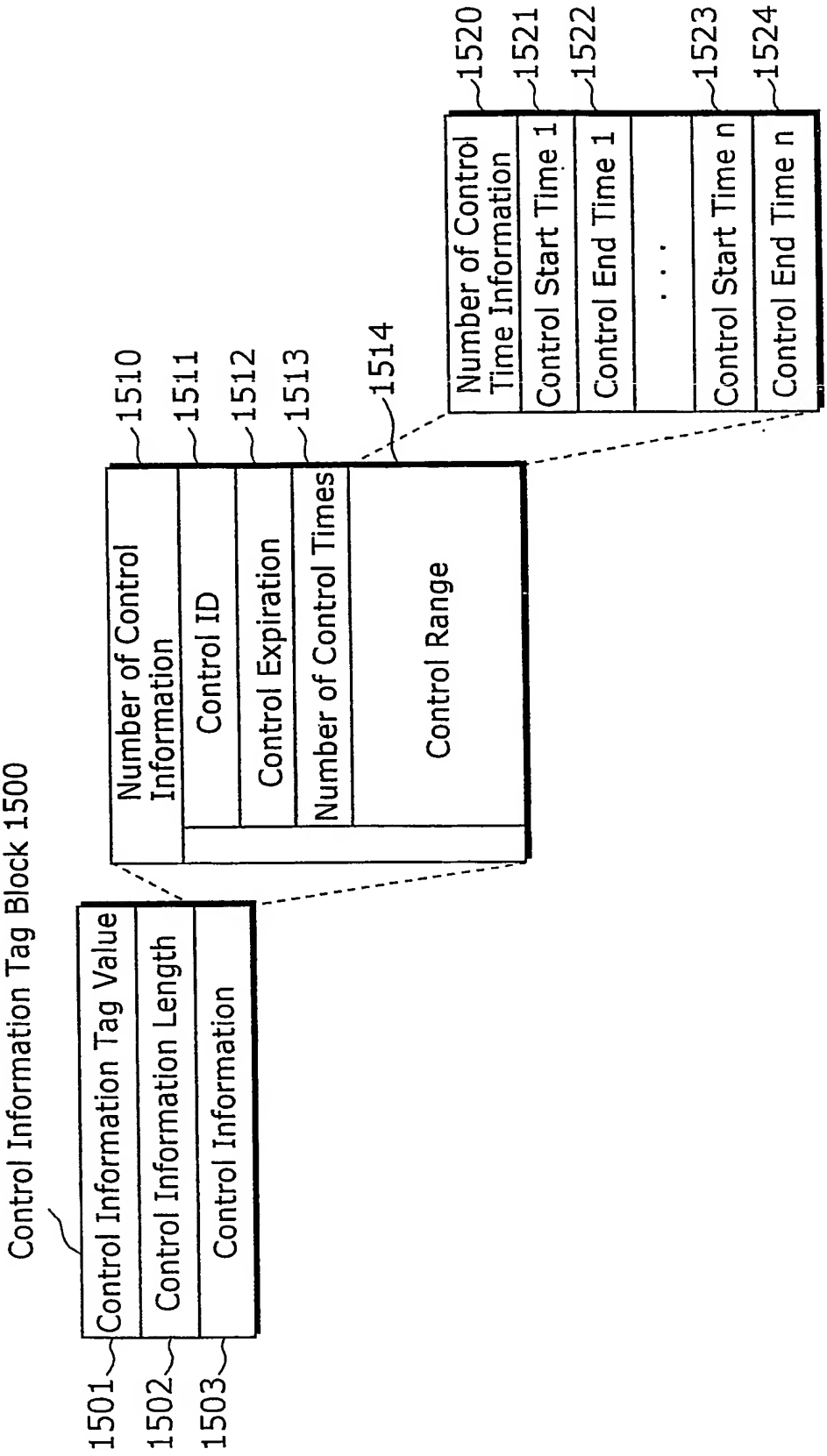

Control Information Tag Block 1500
Control Information Tag Value
Control Information Length
Control Information
1501
1502
1503
Number of Control Information
Control ID
Control Expiration
Number of Control Times
Control Range
1510
1511
1512
1513
1514
Number of Control Time Information
Control Start Time 1
Control End Time 1
. . .
Control Start Time n
Control End Time n
1520
1521
1522
1523
1524

FIG. 16

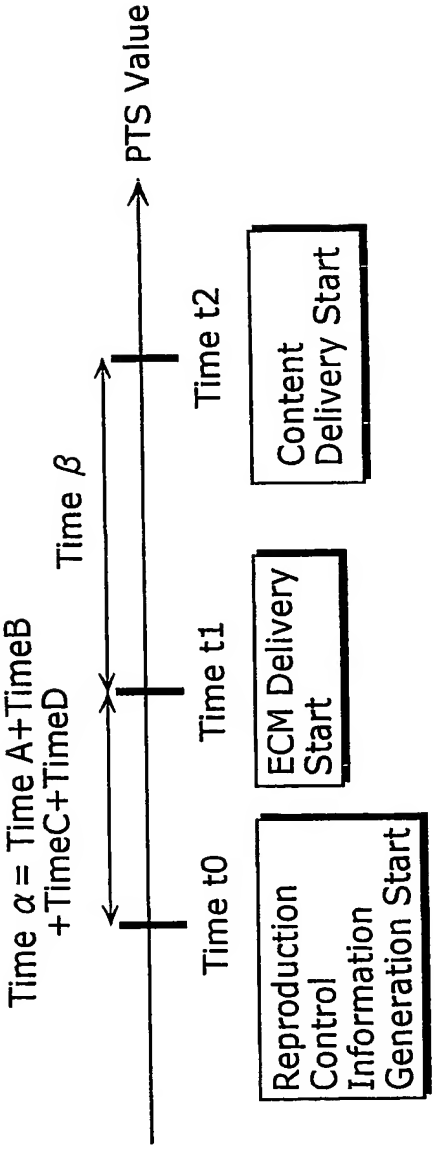

PTS Value
Time t0
Time t1
Time t2
Time α = Time A+TimeB +TimeC+TimeD
Time β
Reproduction Control Information Generation Start
ECM Delivery Start
Content Delivery Start

FIG. 17

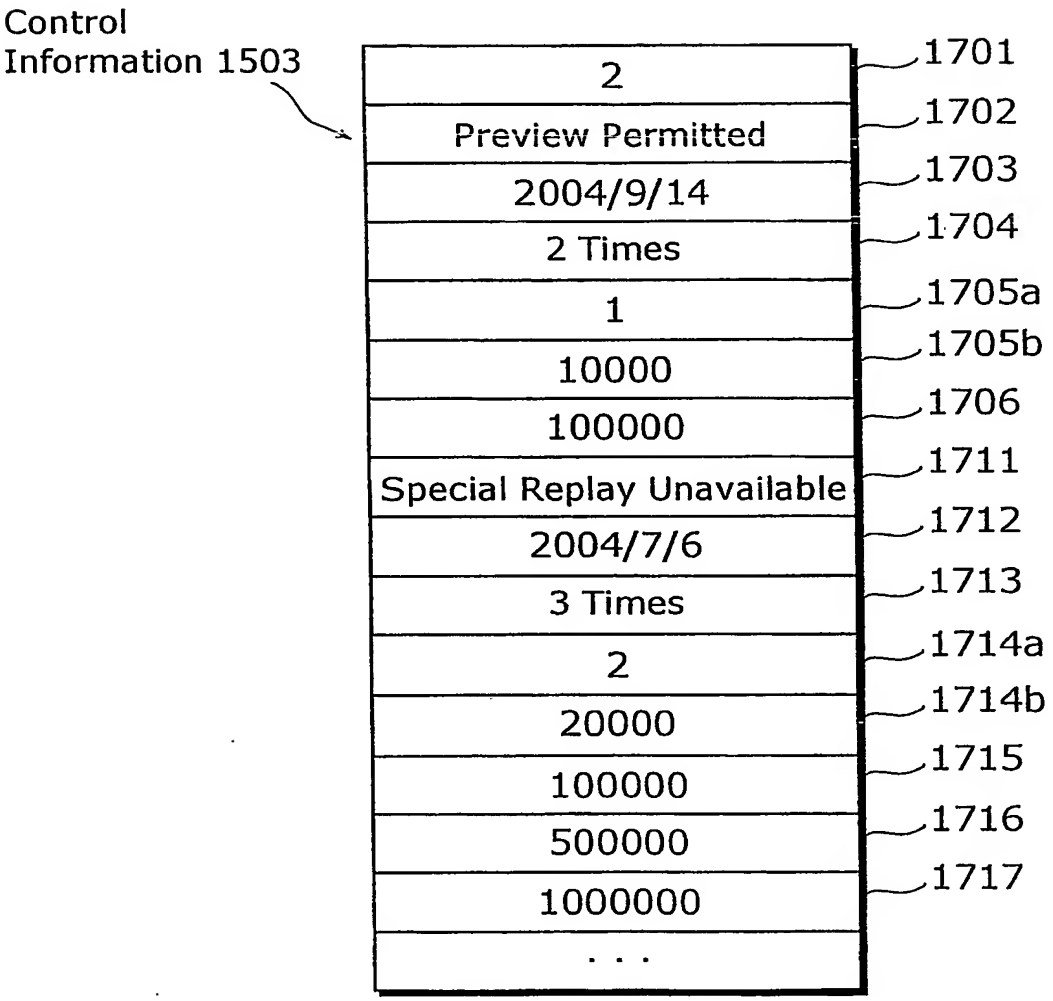

Control
Information 1503
2
Preview Permitted
2004/9/14
2 Times
1
10000
100000
Special Replay Unavailable
2004/7/6
3 Times
2
20000
100000
500000
1000000
. . .
1701
1702
1703
1704
1705a
1705b
1706
1711
1712
1713
1714a
1714b
1715
1716
1717

FIG. 18

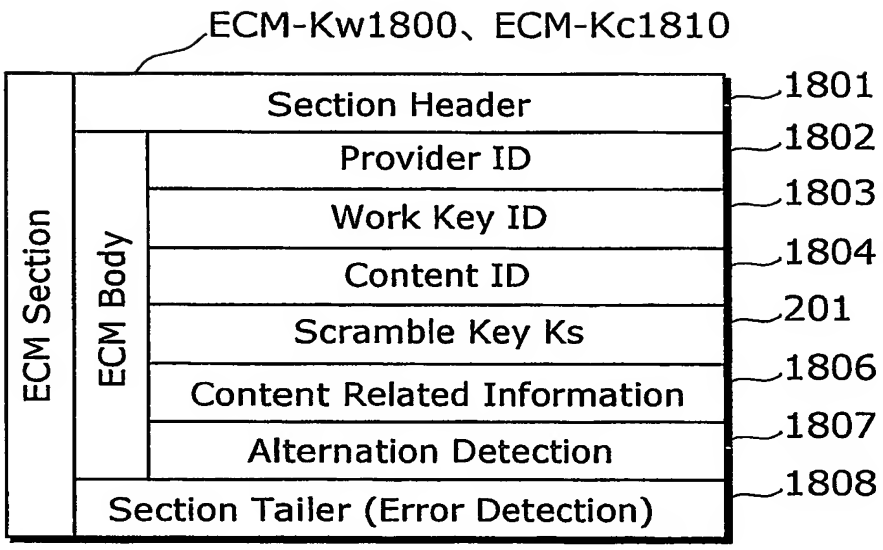

ECM-Kw1800、ECM-Kc1810
ECM Section
ECM Body
Section Header
Provider ID
Work Key ID
Content ID
Scramble Key Ks
Content Related Information
Alternation Detection
Section Tailer (Error Detection)
1801
1802
1803
1804
201
1806
1807
1808

FIG. 19

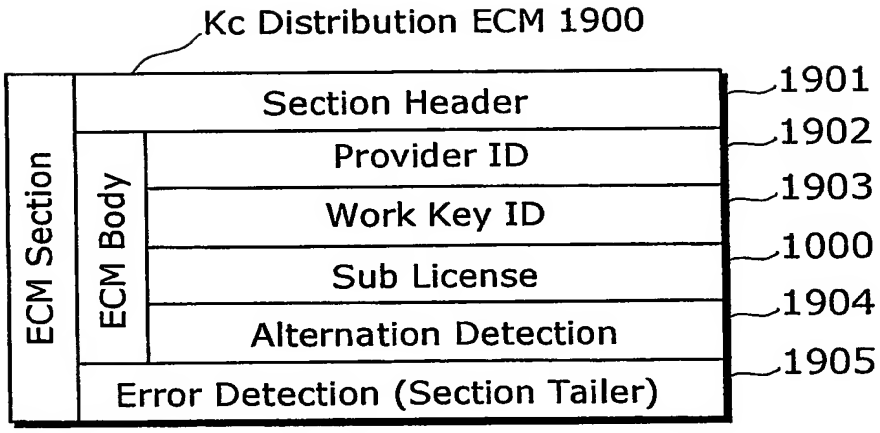

Kc Distribution ECM 1900
ECM Section
ECM Body
Section Header
Provider ID
Work Key ID
Sub License
Alternation Detection
Error Detection (Section Tailer)
1901
1902
1903
1000
1904
1905

FIG. 20

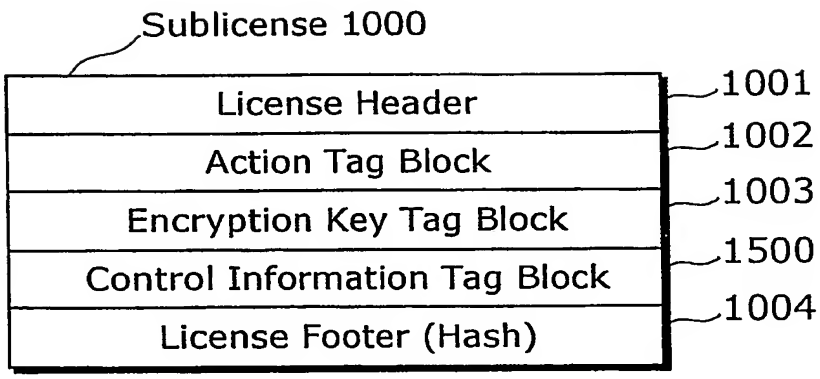

Sublicense 1000
License Header
Action Tag Block
Encryption Key Tag Block
Control Information Tag Block
License Footer (Hash)
1001
1002
1003
1500
1004

FIG. 21

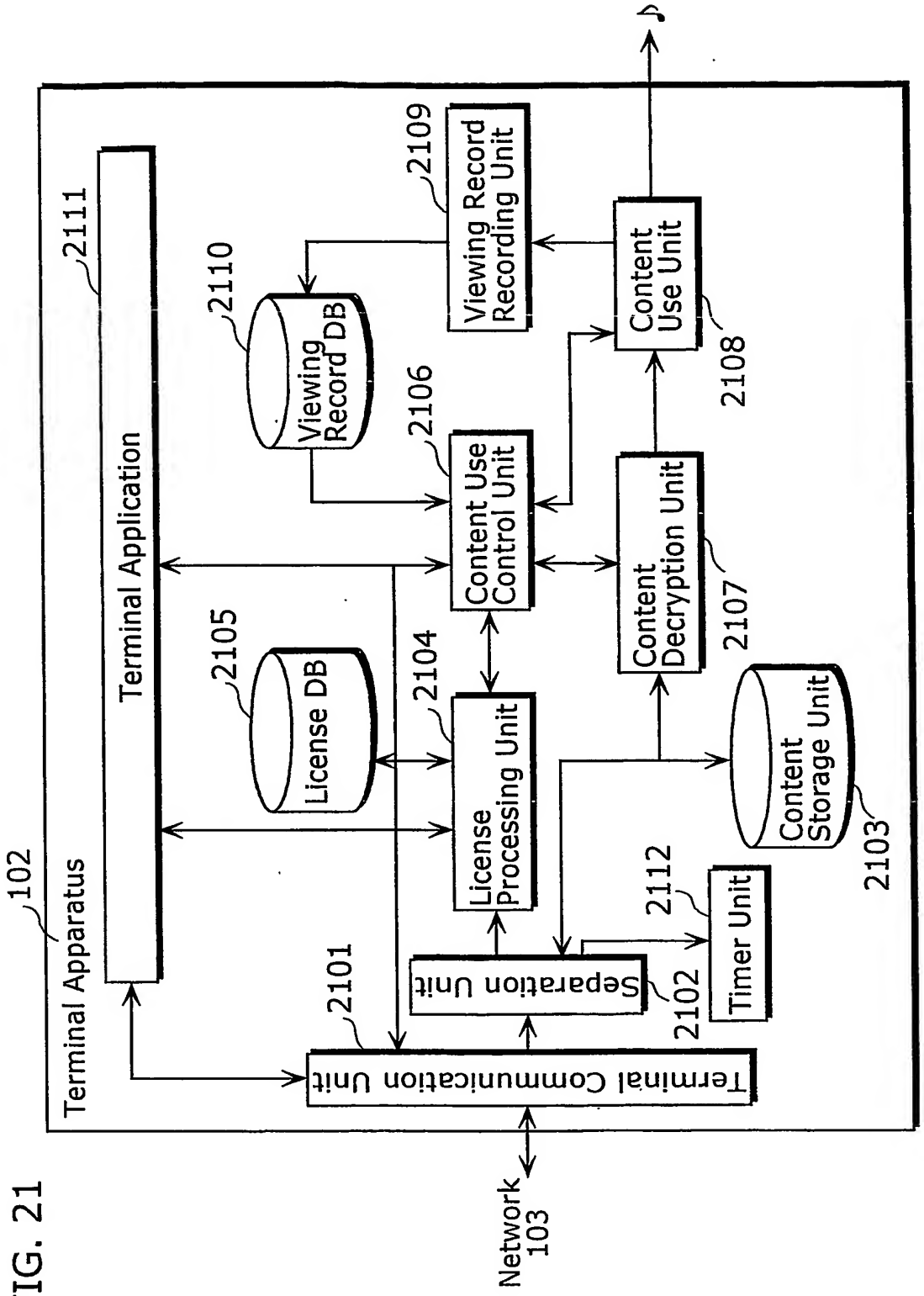

102
Terminal Apparatus
Terminal Application
2111
Terminal Communication Unit
2101
Separation Unit
2102
Timer Unit
2112
License Processing Unit
2104
License DB
2105
Content Use Control Unit
2106
Viewing Record DB
2110
Viewing Record Recording Unit
2109
Content Decryption Unit
2107
Content Use Unit
2108
Content Storage Unit
2103
Network
103

FIG. 22

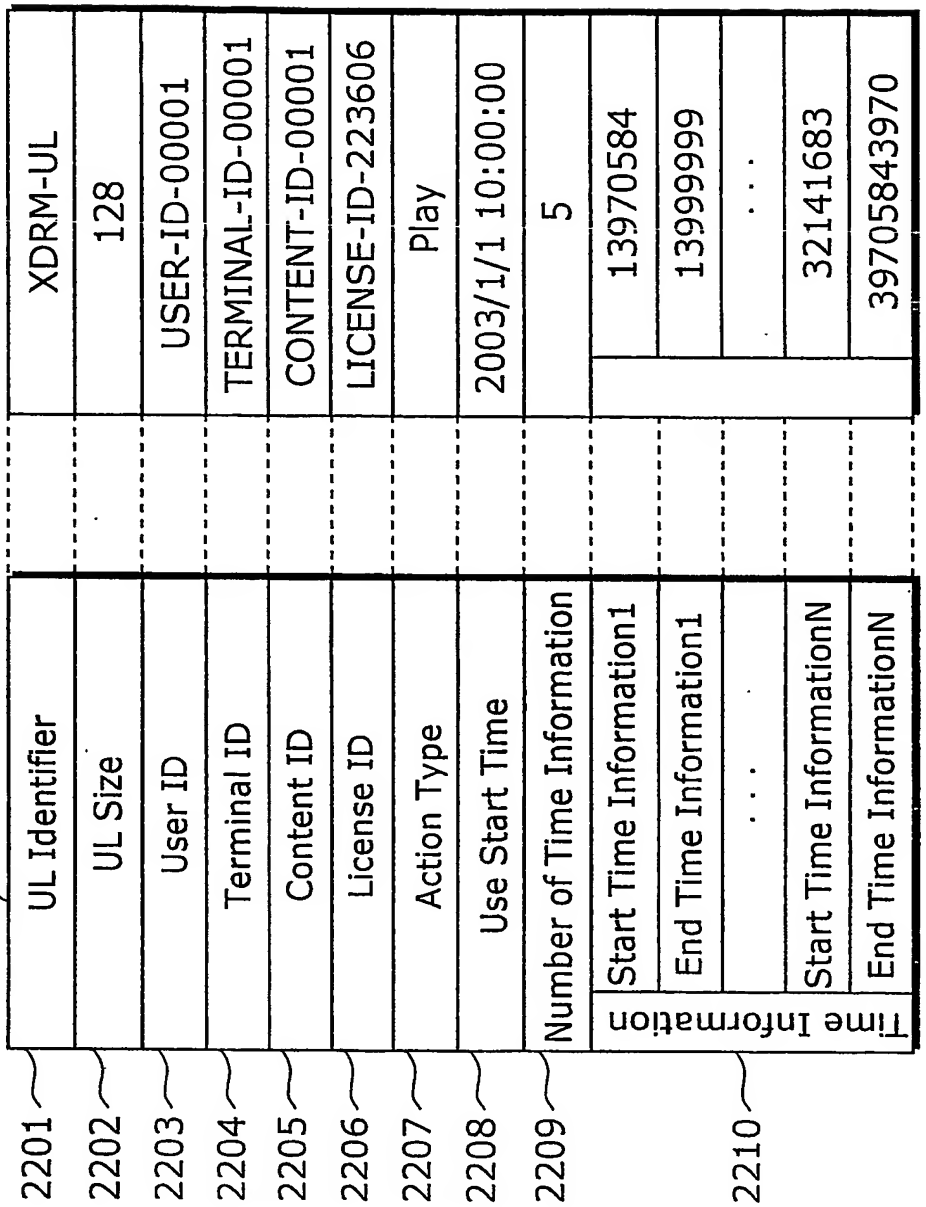

UL2200
UL Identifier
XDRM-UL
UL Size
128
User ID
USER-ID-00001
Terminal ID
TERMINAL-ID-00001
Content ID
CONTENT-ID-00001
License ID
LICENSE-ID-223606
Action Type
Play
Use Start Time
2003/1/1 10:00:00
Number of Time Information
5
Time Information
Start Time Information1
13970584
End Time Information1
13999999
. . .
. . .
Start Time InformationN
32141683
End Time InformationN
39705843970
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210

FIG. 23

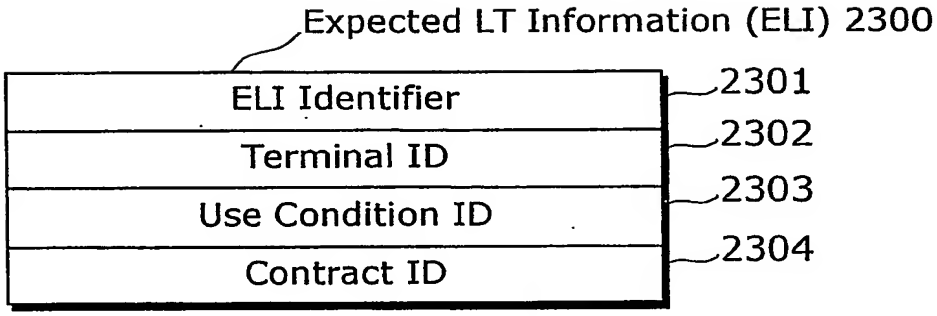

Expected LT Information (ELI) 2300
ELI Identifier
Terminal ID
Use Condition ID
Contract ID
2301
2302
2303
2304

FIG. 24

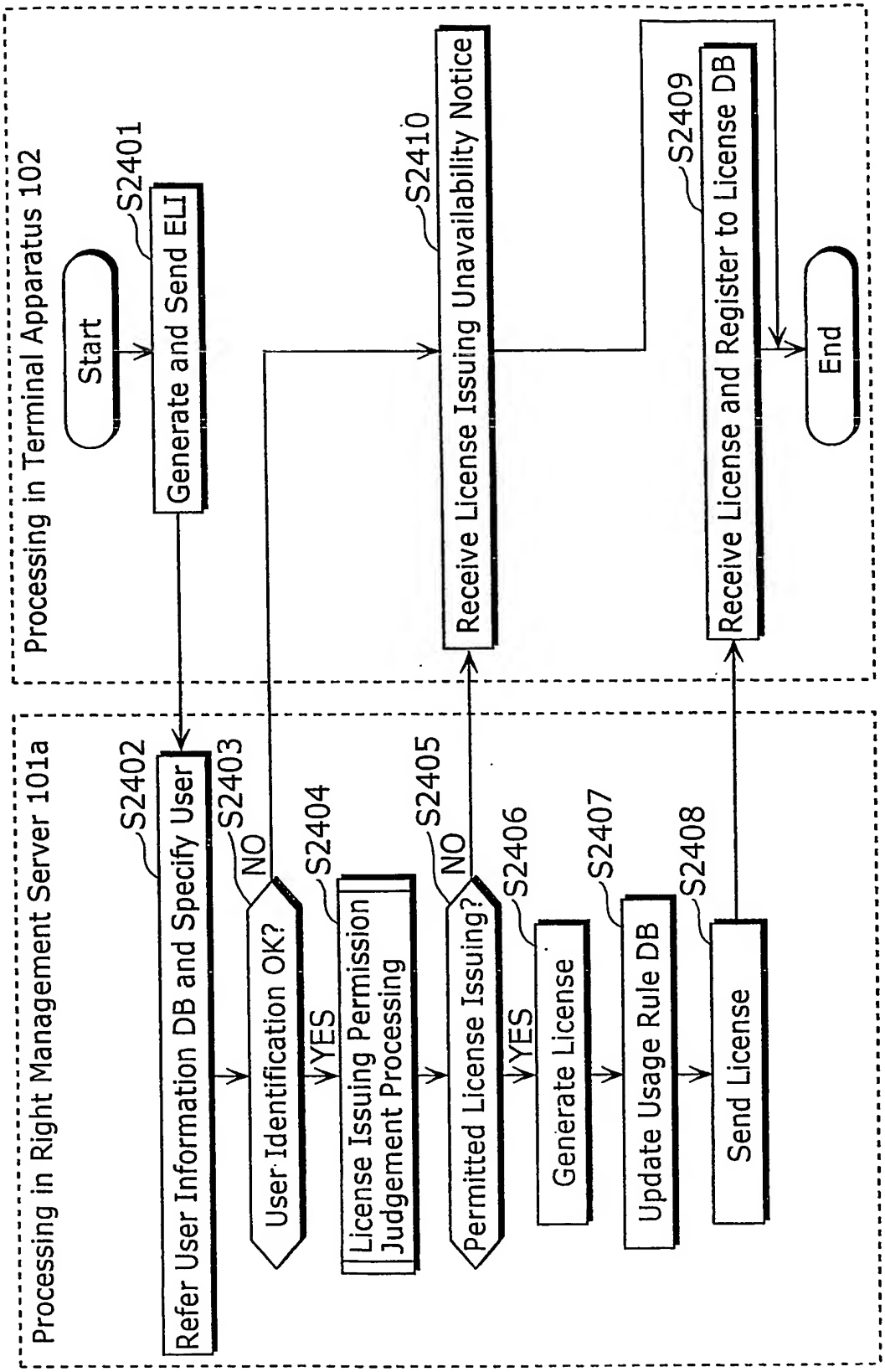

Processing in Terminal Apparatus 102
Start
S2401
Generate and Send ELI
S2410
Receive License Issuing Unavailability Notice
S2409
Receive License and Register to License DB
End
Processing in Right Management Server 101a
S2402
Refer User Information DB and Specify User
S2403
User Identification OK?
NO
YES
S2404
License Issuing Permission Judgement Processing
S2405
Permitted License Issuing?
NO
YES
S2406
Generate License
S2407
Update Usage Rule DB
S2408
Send License

FIG. 25

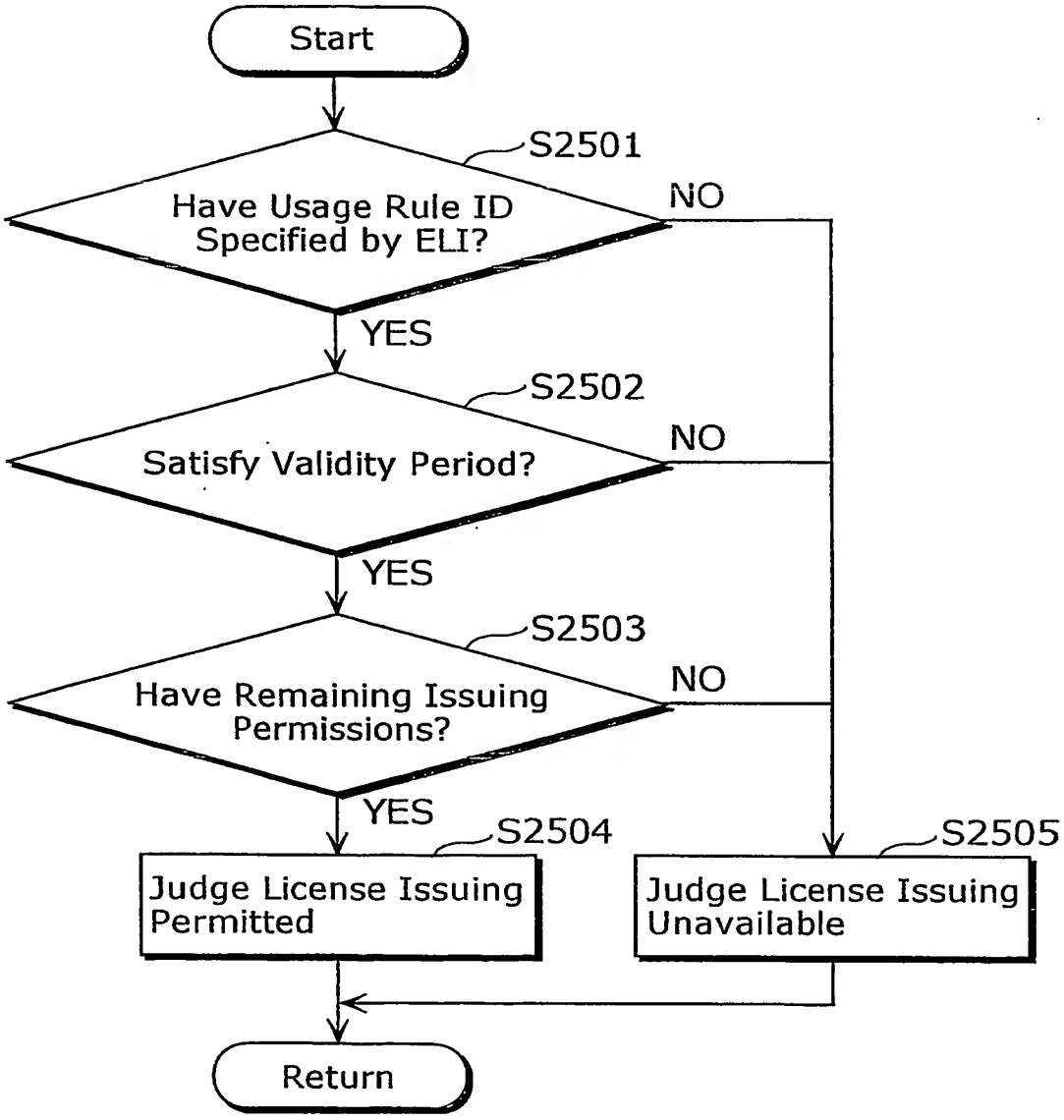

Start
S2501
Have Usage Rule ID Specified by ELI?
NO
YES
S2502
Satisfy Validity Period?
NO
YES
S2503
Have Remaining Issuing Permissions?
NO
YES
S2504
Judge License Issuing Permitted
S2505
Judge License Issuing Unavailable
Return

FIG. 26

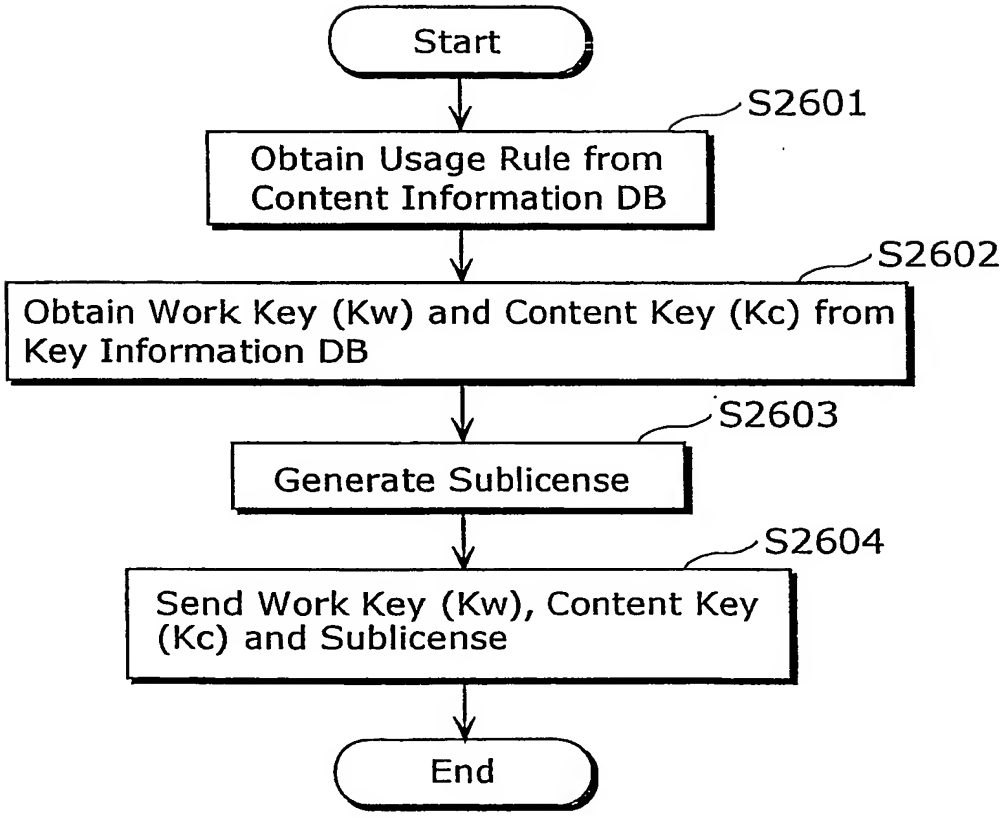

Start
S2601
Obtain Usage Rule from Content Information DB
S2602
Obtain Work Key (Kw) and Content Key (Kc) from Key Information DB
S2603
Generate Sublicense
S2604
Send Work Key (Kw), Content Key (Kc) and Sublicense
End

FIG. 27

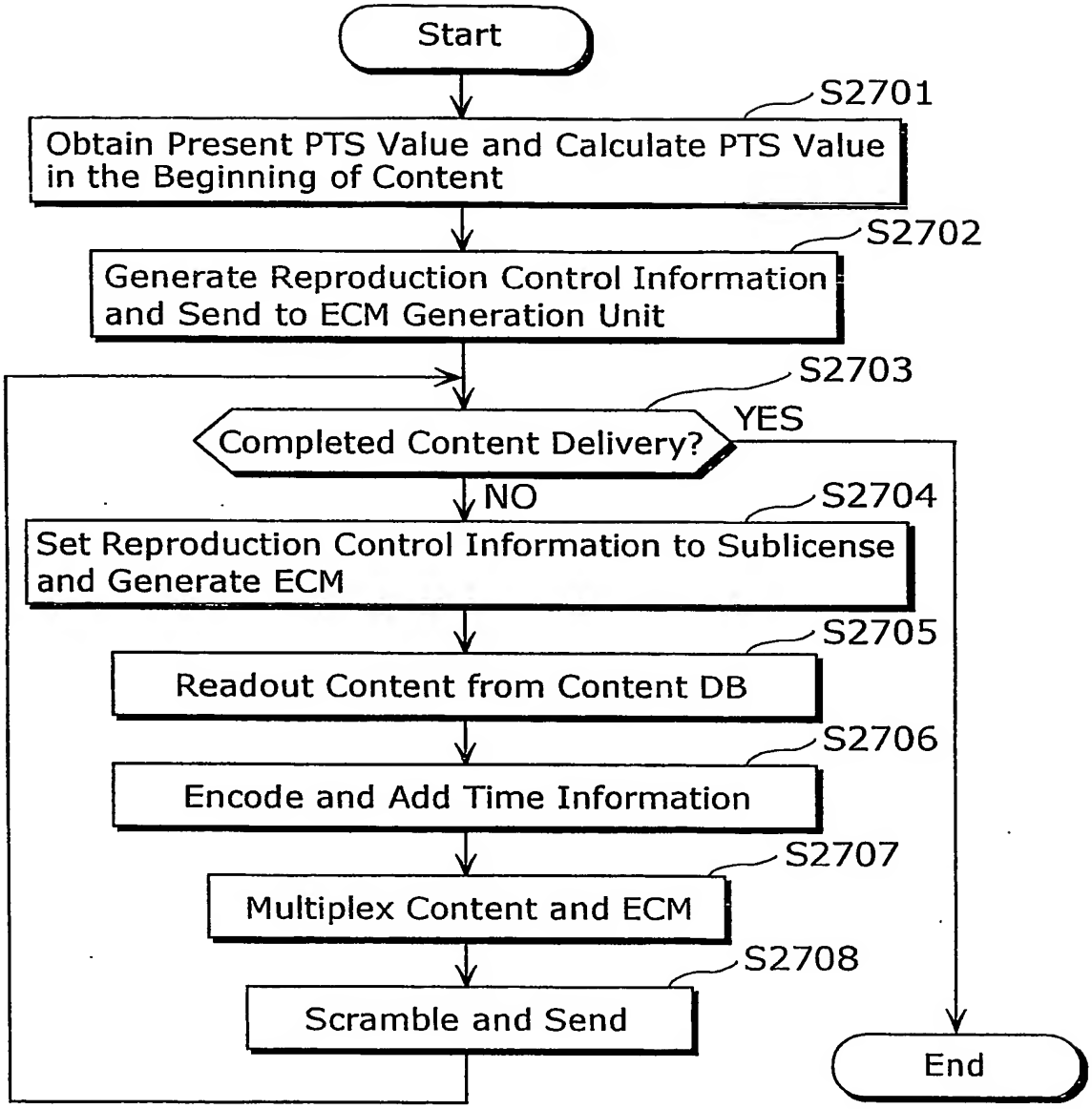

Start
S2701
Obtain Present PTS Value and Calculate PTS Value in the Beginning of Content
S2702
Generate Reproduction Control Information and Send to ECM Generation Unit
S2703
Completed Content Delivery?
YES
NO
S2704
Set Reproduction Control Information to Sublicense and Generate ECM
S2705
Readout Content from Content DB
S2706
Encode and Add Time Information
S2707
Multiplex Content and ECM
S2708
Scramble and Send
End

FIG. 28

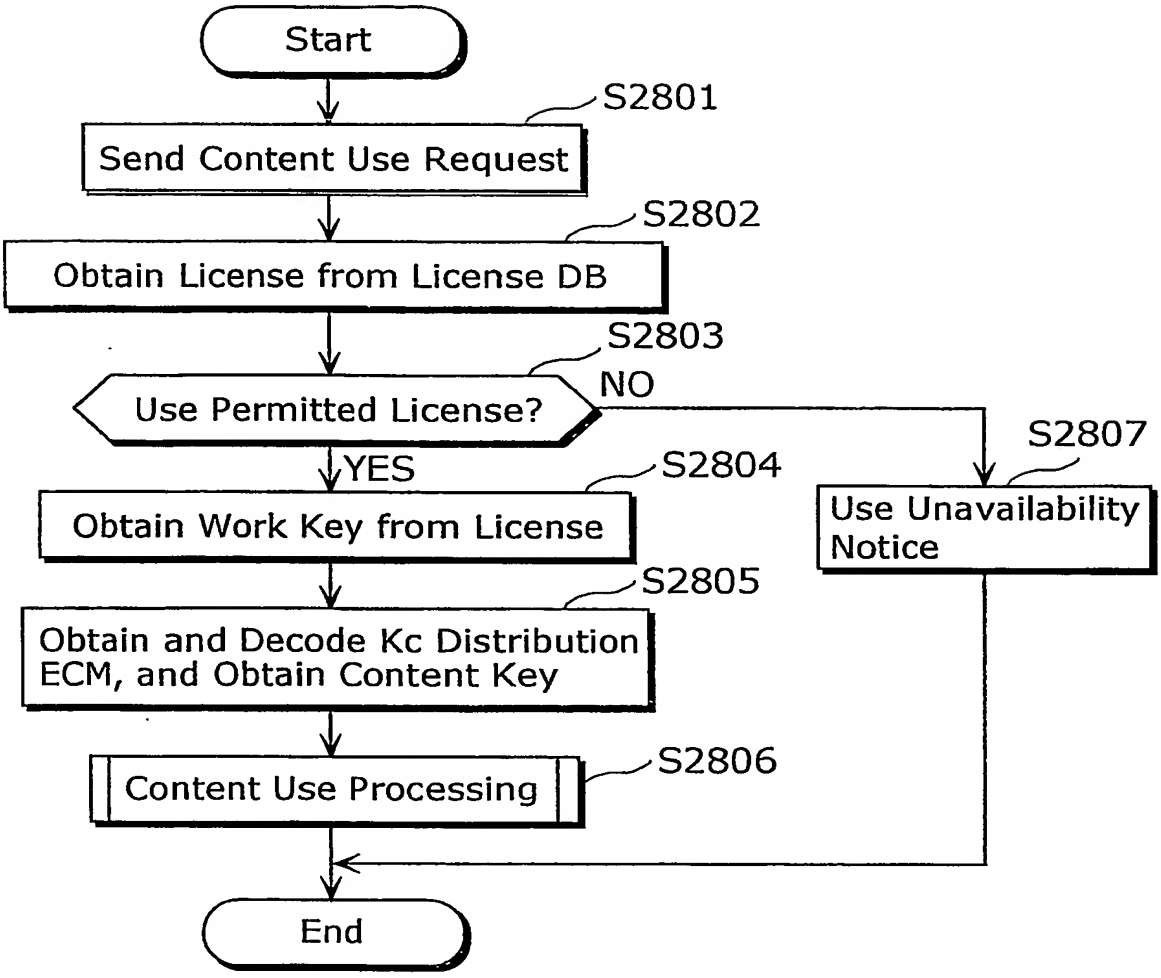

Start
S2801
Send Content Use Request
S2802
Obtain License from License DB
S2803
Use Permitted License?
NO
S2807
Use Unavailability Notice
YES
S2804
Obtain Work Key from License
S2805
Obtain and Decode Kc Distribution ECM, and Obtain Content Key
S2806
Content Use Processing
End

FIG. 29

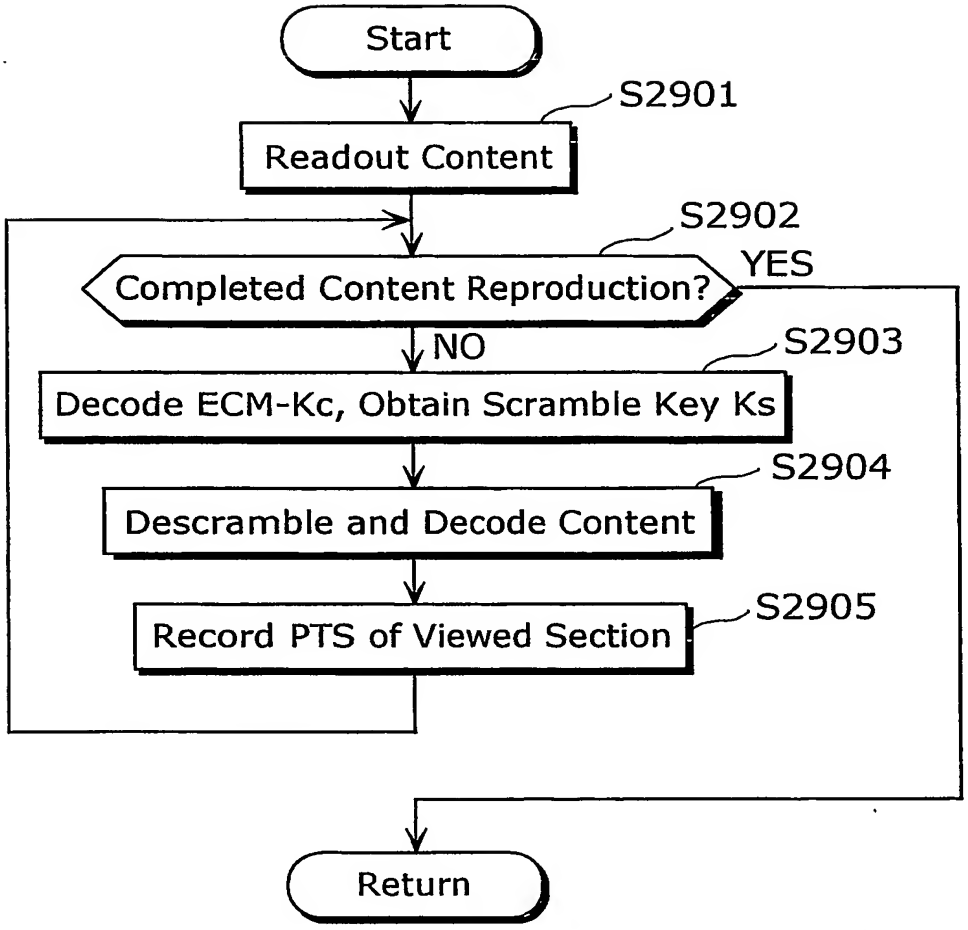

Start
S2901
Readout Content
S2902
Completed Content Reproduction?
YES
NO
S2903
Decode ECM-Kc, Obtain Scramble Key Ks
S2904
Descramble and Decode Content
S2905
Record PTS of Viewed Section
Return

FIG. 30

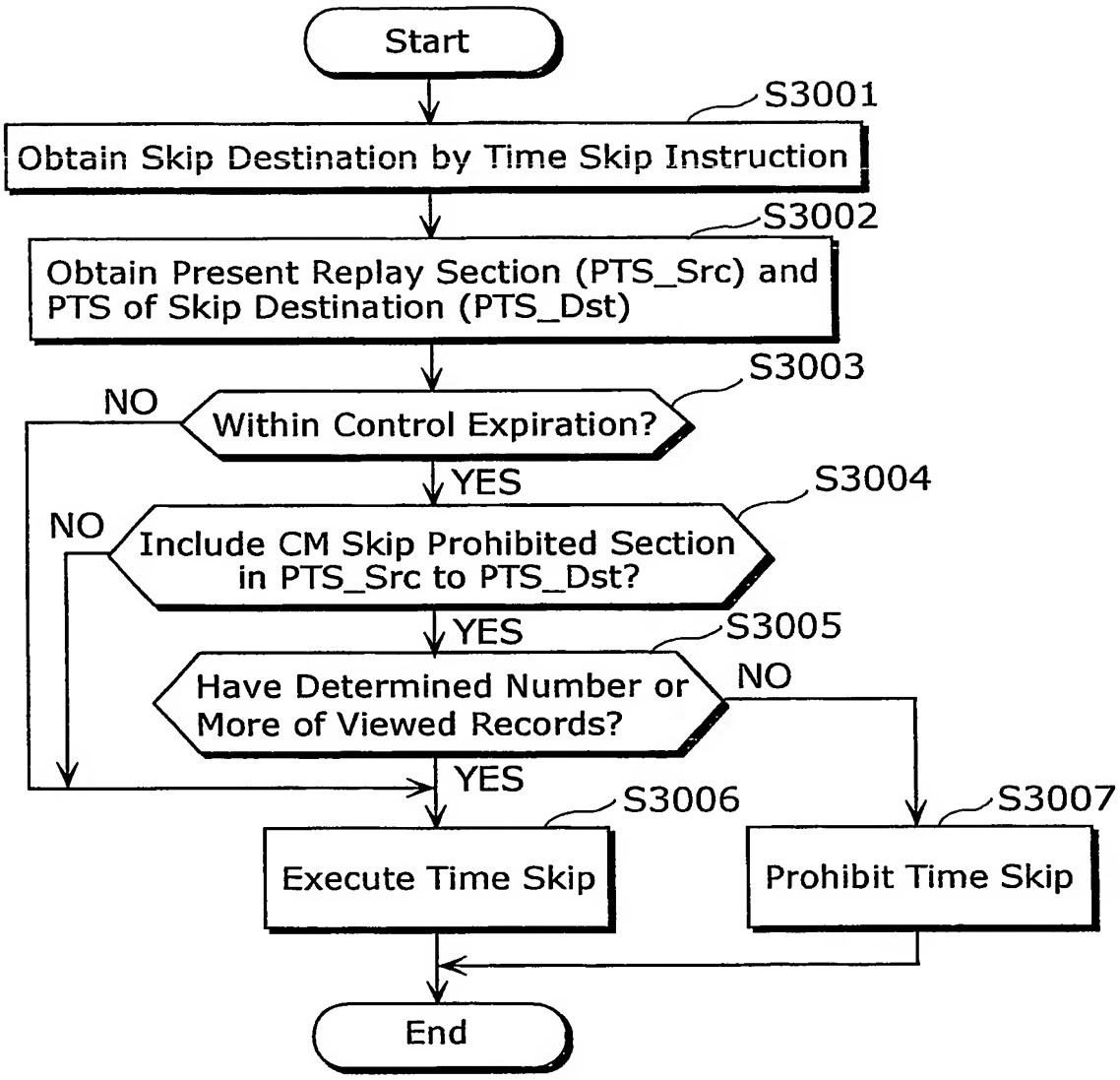

Start
S3001
Obtain Skip Destination by Time Skip Instruction
S3002
Obtain Present Replay Section (PTS_Src) and PTS of Skip Destination (PTS_Dst)
S3003
NO
Within Control Expiration?
YES
S3004
NO
Include CM Skip Prohibited Section in PTS_Src to PTS_Dst?
YES
S3005
Have Determined Number or More of Viewed Records?
NO
YES
S3006
S3007
Execute Time Skip
Prohibit Time Skip
End

FIG. 31

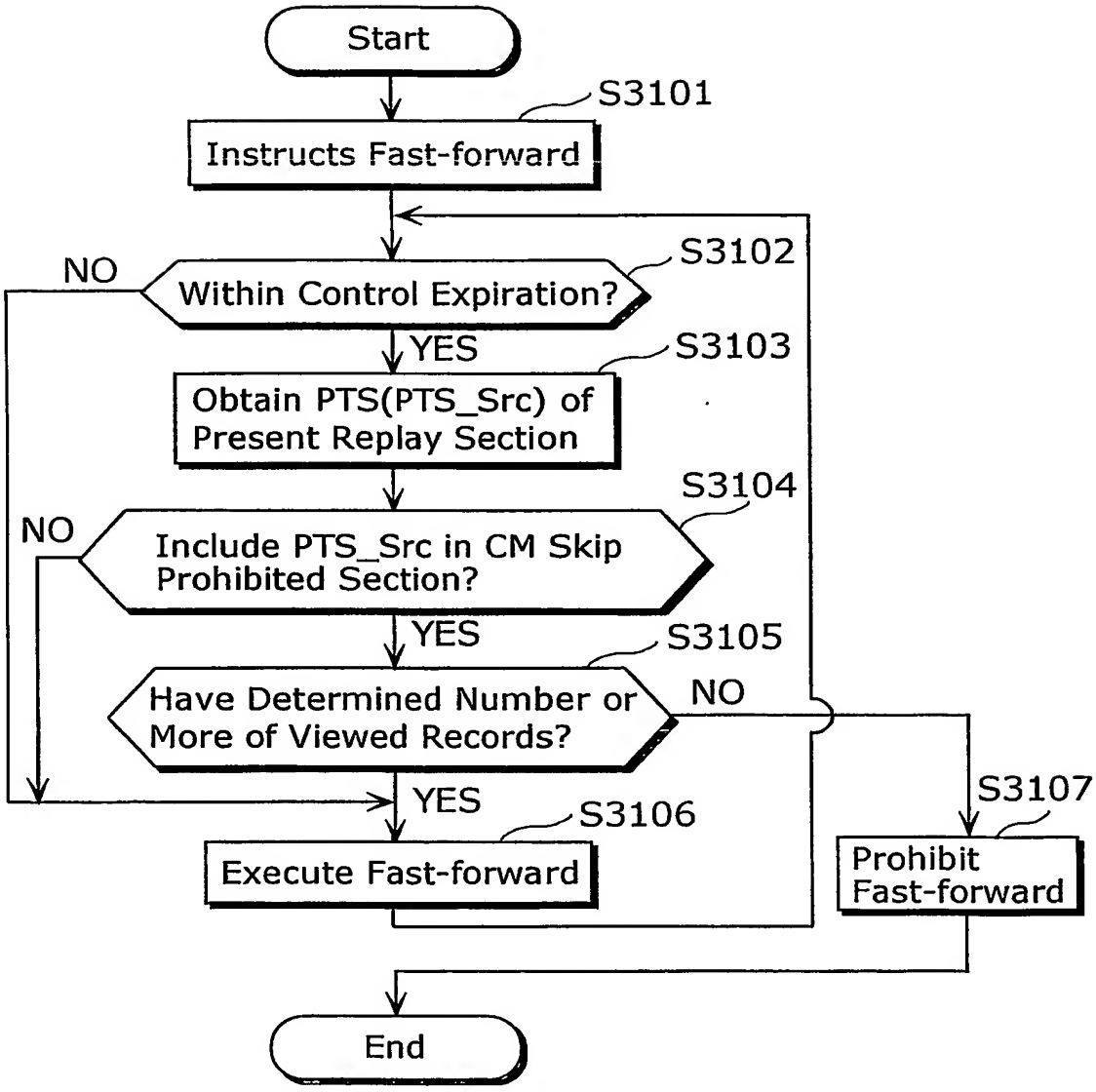
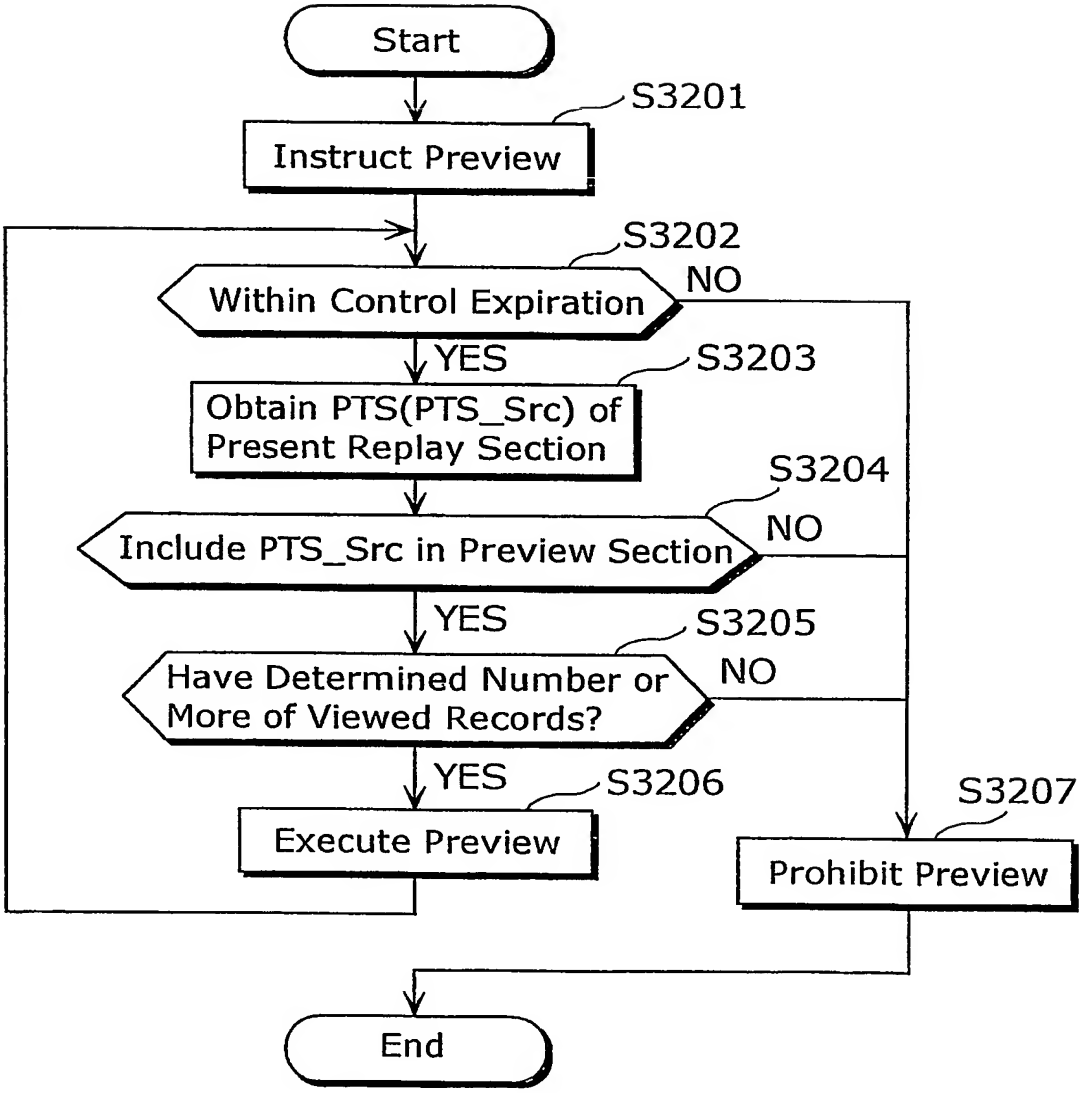

Start
S3101
Instructs Fast-forward
S3102
NO
Within Control Expiration?
YES
S3103
Obtain PTS(PTS_Src) of Present Replay Section
S3104
NO
Include PTS_Src in CM Skip Prohibited Section?
YES
S3105
Have Determined Number or More of Viewed Records?
NO
YES
S3106
Execute Fast-forward
S3107
Prohibit Fast-forward
End

FIG. 32


Start
S3201
Instruct Preview
S3202
Within Control Expiration
NO
YES
S3203
Obtain PTS(PTS_Src) of Present Replay Section
S3204
Include PTS_Src in Preview Section
NO
YES
S3205
Have Determined Number or More of Viewed Records?
NO
YES
S3206
Execute Preview
S3207
Prohibit Preview
End